

REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 20, 28, 34, 39, 40, and 45 are amended. Claims 1-47 are pending in this application.

The Specification

The Specification has been amended to correct a typographical error discovered by Applicant.

35 U.S.C. § 112

Claims 1-12 and 14-47 stand rejected under 35 U.S.C. §112, first paragraph. In the March 21, 2005 Office Action at p. 3, it was asserted that:

The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention commensurate in scope with these claims. The limitation “converting the number to an element of the Jacobian of the curve” covers a much broader spectrum of conversion techniques (including all elliptic curve methods) that is not enabled by the instant specification.

Applicant respectfully disagrees and submits that claims 1-12 and 14-47 comply with 35 U.S.C. §112, first paragraph.

In the March 21, 2005 Office Action at pp. 2-3, it appears that claims 1-12 and 14-47 are rejected under 35 U.S.C. §112, first paragraph as not being enabled, whereas the more-detailed claim 13 is not rejected under 35 U.S.C. §112, first paragraph. Applicant respectfully submits that, in light of the more-detailed claim 13 being admitted as enabled in the March 21, 2005 Office Action, the claims including broader language are also enabled. MPEP §2164.01(b) recites in part:

As long as the specification discloses at least one method for making and using the claimed invention that bears a reasonable correlation to the entire scope of the claim, then the enablement requirement of 35 U.S.C. 112 is satisfied. *In re Fisher*, 427 F.2d 833, 839, 166 USPQ 18, 24 (CCPA 1970). Failure to disclose other methods by which the claimed invention may be made does not render a claim invalid under 35 U.S.C. 112. *Spectra-Physics, Inc. v. Coherent, Inc.*, 827 F.2d 1524, 1533, 3 USPQ2d 1737, 1743 (Fed. Cir.), *cert. denied*, 484 U.S. 954 (1987).

Applicant respectfully submits that at least one such method has been disclosed in the specification, and thus that the claims are valid under 35 U.S.C. §112, first paragraph.

Accordingly, for at least these reasons, Applicant respectfully submits that claims 1-12 and 14-47 comply with 35 U.S.C. §112, first paragraph.

Claim 39 stands stand rejected under 35 U.S.C. §112, second paragraph. Claim 39 has been amended to correct the antecedent basis issue noted by the examiner. Applicant respectfully submits that amended claim 39 complies with 35 U.S.C. §112, second paragraph.

Applicant respectfully requests that the §112 rejections be withdrawn.

35 U.S.C. § 101

Claims 20-47 stand rejected under 35 U.S.C. §101 as not being tangible. Independent claims 20, 28, and 34 have been amended to clarify that claims 20, 28, and 34 comply with 35 U.S.C. §101. Given that claims 21-27 depend from claim 20, claims 29-33 depend from claim 28, and claims 35-39 depend from claim 34, Applicant respectfully submits that claims 20-39 comply with 35 U.S.C. §101.

With respect to claims 40-47, each of claims 40-47 is directed to a system. In the case of independent claim 40, the system includes an input module and an encryption module, and in the case of independent claim 45, the system includes an input module and a decryption module. Applicant respectfully submits that a system including multiple modules complies with 35 U.S.C. §101, and it is unclear how such a multiple-module system can be viewed as not being tangible in the March 21, 2005 Office Action. Given that claims 41-44 depend from claim 40, and claims 46-47 depend from claim 45, claims 40-47 comply with 35 U.S.C. §101.

For at least these reasons, Applicant respectfully submits that claims 20-47 comply with 35 U.S.C. §101.

Applicant respectfully requests that the §101 rejections be withdrawn.

35 U.S.C. § 102

Claims 28, 30, 31, 34, 35, 40, 43, 45, and 46 stand rejected under 35 U.S.C. §102(b) as being unpatentable over “Algebraic Aspects of Cryptography” to Koblitz (hereinafter “Koblitz”). Applicant respectfully submits that claims 28, 30, 31, 34, 35, 40, 43, 45, and 46 are not anticipated by Koblitz.

With respect to claim 28, claim 28 recites:

A computer-implemented encryption method, comprising:
encrypting a message using a secret; and
wherein the secret comprises the order of a group of points on
the Jacobian.

Applicant respectfully submits that no such method is disclosed in Koblitz.

Applicant respectfully submits that Koblitz does not disclose that the secret to be used to encrypt a message comprises the order of a group of points on the

Jacobian as recited in claim 28. Although Koblitz mentions the order of the jacobian of a curve C (see, p. 148), there is no mention that the secret used to encrypt a message is the order of a group of points on the jacobian. Applicant respectfully submits that there is no disclosure in the mentioning of the order of the jacobian of a curve in Koblitz on p. 148, or elsewhere in Koblitz, that a secret to be used to encrypt a message comprises the order of a group of points on the Jacobian as recited in claim 28.

Accordingly, for at least these reasons, Applicant respectfully submits that claim 28 is allowable over Koblitz.

With respect to claims 30 and 31, given that claims 30 and 31 depend from claim 28, Applicant respectfully submits that claims 30 and 31 are likewise allowable over Koblitz for at least the reasons discussed above with respect to claim 28.

With respect to claim 34, Applicant respectfully submits that, analogous to the discussion above regarding claim 28, Koblitz does not disclose decrypting a message using a secret and wherein the secret comprises the order of a group of points on a Jacobian of a curve as recited in claim 34. Accordingly, for at least these reasons, Applicant respectfully submits that claim 34 is allowable over Koblitz.

With respect to claim 35, given that claim 35 depends from claim 34, Applicant respectfully submits that claim 35 is likewise allowable over Koblitz for at least the reasons discussed above with respect to claim 34.

With respect to claim 40, Applicant respectfully submits that, analogous to the discussion above regarding claim 28, Koblitz does not disclose an encryption

module, communicatively coupled to the input module, to convert the plaintext message to ciphertext based on both a curve and a secret that is the order of a group of points on a Jacobian of the curve as recited in claim 40. Accordingly, for at least these reasons, Applicant respectfully submits that claim 40 is allowable over Koblitz.

With respect to claim 43, given that claim 43 depends from claim 40, Applicant respectfully submits that claim 43 is likewise allowable over Koblitz for at least the reasons discussed above with respect to claim 40.

With respect to claim 45, Applicant respectfully submits that, analogous to the discussion above regarding claim 28, Koblitz does not disclose a decryption module, communicatively coupled to the input module, to convert the ciphertext to a plaintext message based on both a curve and a secret that is the order of a group of points on a Jacobian of the curve as recited in claim 45. Accordingly, for at least these reasons, Applicant respectfully submits that claim 45 is allowable over Koblitz.

With respect to claim 46, given that claim 46 depends from claim 45, Applicant respectfully submits that claim 46 is likewise allowable over Koblitz for at least the reasons discussed above with respect to claim 45.

Applicant respectfully requests that the §102 rejections be withdrawn.

35 U.S.C. § 103

Claims 1-27 and 39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Koblitz in view of “Applied Cryptography” to Schneier (hereinafter “Schneier”) and U.S. Patent No. 6,845,395 to Blumenau et al.

(hereinafter “Blumenau”). Applicant respectfully submits that claims 1-27 and 39 are not obvious over Koblitz in view of Schneier and Blumenau.

With respect to claim 1, claim 1 recites:

One or more computer-readable media having stored thereon a plurality of instructions for generating a product identifier, wherein the plurality of instructions, when executed by one or more processors, causes the one or more processors to perform the following acts:

- receiving a value;
- padding the received value using a recognizable pattern;
- converting the padded value to a number represented by a particular number of bits;
- converting the number to an element of the Jacobian of a curve;
- raising the element to a particular power;
- compressing the result of raising the element to the particular power; and
- outputting, as the product identifier, the compressed result.

Applicant respectfully submits that no such generating a product identifier is disclosed or suggested by Koblitz in view of Schneier and Blumenau.

Koblitz is cited in the March 21 Office Action at p. 6 as disclosing the converting the number to an element of the Jacobian of a curve and raising the element to a particular power of claim 1. Applicant respectfully disagrees and submits that such converting and raising is not disclosed or suggested by Koblitz. The cited portion of Koblitz discusses hyperelliptic cryptosystems including different hyperelliptic curves C . However, in claim 1, a value is converted to an element of the Jacobian of a curve, the element is raised to a particular power, and a result is output. The discussion of hyperelliptic cryptosystems in Koblitz includes no discussion or mention of converting a number to an element of the Jacobian of a curve. Although the cited portions of Koblitz discuss the jacobian of

a curve and the number of points on the jacobian of the curve, there is no discussion or mention that a number is converted to an element of the Jacobian of a curve.

Furthermore, not only is there no discussion or mention that a number is converted to an element of the Jacobian of a curve, there is no discussion or mention of raising that element to a particular power as recited in claim 1. Although the cited portions of Koblitz discuss the jacobian of a curve and the number of points on the jacobian of the curve, there is no discussion or mention that such an element is raised to a particular power as recited in claim 1.

Schneier and Blumenau are not cited as curing, and do not cure, these deficiencies of Koblitz. Accordingly, for at least these reasons, Applicant respectfully submits that claim 1 is allowable over Koblitz in view of Schneier and Blumenau.

With respect to claims 2-12, given that claims 2-12 depend from claim 1, Applicant respectfully submits that claims 2-12 are likewise allowable over Koblitz in view of Schneier and Blumenau for at least the reasons discussed above with respect to claim 1.

With respect to claim 13, claim 13 depends from claim 1 and Applicant respectfully submits that claim 13 is allowable over Koblitz in view of Schneier and Blumenau for at least the reasons discussed above with respect to claim 1. Furthermore, claim 13 recites:

One or more computer-readable media as recited in claim 12, wherein converting the number to an element of the Jacobian of a curve comprises:

determining a value $a(x)$, wherein the value $a(x)$ is a monic irreducible polynomial of degree g ;

determining a value $b(x)$, wherein the value $b(x)$ is a square root of $f(x)$ modulo $a(x)$ of degree less than $a(x)$; and
using, as the element of the Jacobian of the curve, the values $a(x)$ and $b(x)$.

Applicant respectfully submits that no such determining and using is disclosed or suggested in Koblitz in view of Schneier and Blumenau.

Koblitz is cited in the March 21 Office Action at p. 6 as disclosing the determining and using of claim 1. Although Koblitz discusses the jacobian of a curve and the number of points on the jacobian of the curve, as well as numerous equations for determining various values, there is no discussion or mention of determining two values $a(x)$ and $b(x)$ in the manner recited in claim 13, much less of using such values as the element of the Jacobian of the curve as recited in claim 13. Without any discussion or mention of determining two values in the manner recited in claim 13, and without any discussion or mention of using the two determined values in the manner recited in claim 13, Applicant respectfully submits that Koblitz cannot disclose or suggest the determining and using of claim 13.

Schneier and Blumenau are not cited as curing, and do not cure, these deficiencies of Koblitz. Accordingly, for at least these reasons, Applicant respectfully submits that claim 13 is allowable over Koblitz in view of Schneier and Blumenau.

With respect to claim 14, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Koblitz in view of Schneier and Blumenau do not disclose or suggest raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on an element of a Jacobian of a curve as recited in claim 14. Accordingly, for at least these

reasons, Applicant respectfully submits that claim 14 is allowable over Koblitz in view of Schneier and Blumenau.

With respect to claims 15, 16, 18, and 19, given that claims 15, 16, 18, and 19 depend from claim 14, Applicant respectfully submits that claims 15, 16, 18, and 19 are likewise allowable over Koblitz in view of Schneier and Blumenau for at least the reasons discussed above with respect to claim 14.

With respect to claim 17, claim 17 depends from claim 14 and Applicant respectfully submits that claim 17 is allowable over Koblitz in view of Schneier and Blumenau for at least the reasons discussed above with respect to claim 14. Furthermore, analogous to the discussion above regarding claim 28, Applicant respectfully submits that Koblitz does not disclose or suggest wherein the order of the group of points on the Jacobian of the curve is maintained as a secret as recited in claim 17. Schneier and Blumenau are not cited as curing, and do not cure, these deficiencies of Koblitz. Accordingly, for at least these reasons, Applicant respectfully submits that claim 17 is allowable over Koblitz in view of Schneier and Blumenau.

With respect to claim 20, Applicant respectfully submits that, analogous to the discussion above regarding claim 28, Koblitz does not disclose or suggest recovering a plaintext message from the encrypted product identifier, wherein the recovering is based on a secret that is the size of a group of points on a Jacobian of a curve as recited in claim 20. Schneier and Blumenau are not cited as curing, and do not cure, these deficiencies of Koblitz. Accordingly, for at least these reasons, Applicant respectfully submits that claim 20 is allowable over Koblitz in view of Schneier and Blumenau.

With respect to claims 21, 22, and 24-27, given that claims 21, 22, and 24-27 depend from claim 20, Applicant respectfully submits that claims 21, 22, and 24-27 are likewise allowable over Koblitz in view of Schneier and Blumenau for at least the reasons discussed above with respect to claim 20.

With respect to claim 23, claim 23 depends from claim 20 and Applicant respectfully submits that claim 23 is allowable over Koblitz in view of Schneier and Blumenau for at least the reasons discussed above with respect to claim 20. Furthermore, similar to the discussion above regarding claim 1, Applicant respectfully submits that Koblitz does not disclose or suggest raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on the size of the group of points on the Jacobian of the curve as recited in claim 23. Schneier and Blumenau are not cited as curing, and do not cure, these deficiencies of Koblitz. Accordingly, for at least these reasons, Applicant respectfully submits that claim 23 is allowable over Koblitz in view of Schneier and Blumenau.

With respect to claim 39, claim 39 depends from claim 34 and Applicant respectfully submits that claim 39 is allowable over Koblitz for at least the reasons discussed above with respect to claim 34. Schneier and Blumenau are not cited as curing, and do not cure, the deficiencies of Koblitz discussed above with respect to claim 34. Accordingly, for at least these reasons, Applicant respectfully submits that claim 39 is allowable over Koblitz in view of Schneier and Blumenau.

Claims 29, 38, 44, and 47 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Koblitz in view of Schneier. Applicant respectfully submits that claims 29, 38, 44, and 47 are not obvious over Koblitz in view of Schneier.

With respect to claim 29, claim 29 depends from claim 28 and Applicant respectfully submits that claim 29 is allowable over Koblitz for at least the reasons discussed above with respect to claim 28. Schneier is not cited as curing, and does not cure, the deficiencies of Koblitz discussed above with respect to claim 28. For at least these reasons, Applicant respectfully submits that claim 29 is allowable over Koblitz in view of Schneier.

Furthermore, analogous to the discussion above regarding claim 1, Applicant respectfully submits that Koblitz in view of Schneier does not disclose or suggest converting the number to an element of the Jacobian of a curve, and raising the element to a particular power as recited in claim 29. Accordingly, for at least these reasons, Applicant respectfully submits that claim 29 is allowable over Koblitz in view of Schneier.

With respect to claim 38, claim 38 depends from claim 34 and Applicant respectfully submits that claim 38 is allowable over Koblitz for at least the reasons discussed above with respect to claim 34. Schneier is not cited as curing, and does not cure, the deficiencies of Koblitz discussed above with respect to claim 34. For at least these reasons, Applicant respectfully submits that claim 38 is allowable over Koblitz in view of Schneier.

Furthermore, Applicant respectfully submits that Koblitz does not disclose or suggest raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on the order of the group of points on the Jacobian of the curve as recited in claim 38. Although Koblitz discusses the jacobian of a curve and the number of points on the jacobian of the curve, as well as numerous equations for determining various values, there

is no discussion or mention of raising a value to a particular exponent, the raising being based at least in part on the order of the group of points on the Jacobian of the curve as recited in claim 38. Without any discussion or mention of such raising, Applicant respectfully submits that Koblitz cannot disclose or suggest raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on the order of the group of points on the Jacobian of the curve as recited in claim 38.

Schneier is not cited as curing, and does not cure, these deficiencies of Koblitz. Accordingly, for at least these reasons, Applicant respectfully submits that claim 38 is allowable over Koblitz in view of Schneier.

With respect to claim 44, claim 44 depends from claim 40 and Applicant respectfully submits that claim 44 is allowable over Koblitz for at least the reasons discussed above with respect to claim 40. Schneier is not cited as curing, and does not cure, the deficiencies of Koblitz discussed above with respect to claim 40. For at least these reasons, Applicant respectfully submits that claim 44 is allowable over Koblitz in view of Schneier.

Furthermore, analogous to the discussion above regarding claim 1, Applicant respectfully submits that Koblitz in view of Schneier does not disclose or suggest converting the number to an element of the Jacobian of the curve, raising the element to a particular power as recited in claim 44. Accordingly, for at least these reasons, Applicant respectfully submits that claim 44 is allowable over Koblitz in view of Schneier.

With respect to claim 47, claim 47 depends from claim 45 and Applicant respectfully submits that claim 47 is allowable over Koblitz for at least the reasons

discussed above with respect to claim 45. Schneier is not cited as curing, and does not cure, the deficiencies of Koblitz discussed above with respect to claim 45. For at least these reasons, Applicant respectfully submits that claim 47 is allowable over Koblitz in view of Schneier.

Furthermore, analogous to the discussion above regarding claim 38, Applicant respectfully submits that Koblitz in view of Schneier does not disclose or suggest raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on the order of the group of points on the Jacobian of the curve as recited in claim 47. Accordingly, for at least these reasons, Applicant respectfully submits that claim 47 is allowable over Koblitz in view of Schneier.

Claims 32, 33, 36, and 37 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Koblitz in view of Blumenau. Applicant respectfully submits that claims 32, 33, 36, and 37 are not obvious over Koblitz in view of Blumenau.

With respect to claims 32 and 33, claims 32 and 33 depend from claim 28 and Applicant respectfully submits that claims 32 and 33 are allowable over Koblitz for at least the reasons discussed above with respect to claim 28. Blumenau is not cited as curing, and does not cure, the deficiencies of Koblitz discussed above with respect to claim 28. Accordingly, for at least these reasons, Applicant respectfully submits that claims 32 and 33 are allowable over Koblitz in view of Blumenau.

With respect to claims 36 and 37, claims 36 and 37 depend from claim 34 and Applicant respectfully submits that claims 36 and 37 are allowable over Koblitz for at least the reasons discussed above with respect to claim 34.

Blumenau is not cited as curing, and does not cure, the deficiencies of Koblitz discussed above with respect to claim 34. Accordingly, for at least these reasons, Applicant respectfully submits that claims 36 and 37 are allowable over Koblitz in view of Blumenau.

Claims 41 and 42 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Koblitz. Applicant respectfully submits that claims 41 and 42 are not obvious over Koblitz. Claims 41 and 42 depend from claim 40 and Applicant respectfully submits that claims 41 and 42 allowable over Koblitz for at least the reasons discussed above with respect to claim 40.

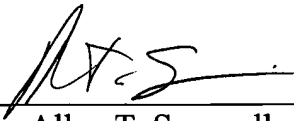
Applicant respectfully requests that the §103 rejections be withdrawn.

Conclusion

Claims 1-47 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 6/21/05

By: 
Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256